1996-09

Automated messaging for the Global Command and Control System: analysis of upgrading communications in the NPS Secure Systems Technology Laboratory (SSTL)

Morrow, Shenae Y.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

AUTOMATED MESSAGING FOR THE GLOBAL COMMAND AND CONTROL SYSTEM: ANALYSIS OF UPGRADING COMMUNICATIONS IN THE NPS SECURE SYSTEMS TECHNOLOGY LABORATORY (SSTL)

by

Shenae Y. Morrow

September, 1996

Principal Advisor: Gary Porter

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1996	Master's Thesis

4. TITLE AND SUBTITLE: **AUTOMATED MESSAGING FOR THE GLOBAL COMMAND AND CONTROL SYSTEM: ANALYSIS OF UPGRADING COMMUNICATIONS IN THE NPS SECURE SYSTEMS TECHNOLOGY LABORATORY (SSTL)**

5. FUNDING NUMBERS

6. AUTHOR(S) Shenae Y. Morrow

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

The Global Command and Control System (GCCS) is currently operational in the Secure Systems Technology Laboratory located in Root Hall at the Naval Postgraduate School. All subsystems of GCCS are operational with the exception of the Automated Message Handling System (AMHS). The SSTL's efforts to obtain an operational GCCS AMHS depends on the future availability of the Automated Defense Information Network (AUTODIN), and the emerging technology of the Defense Message System (DMS). This thesis examines and compares GCCS AMHS and DMS and the implementation requirements for each. This thesis draws the conclusion that DMS is the dominant system over GCCS AMHS and continues to examine the acquisition strategies and costs required to implement the DMS in the SSTL.

14.SUBJECT TERMS			15. NUMBER OF PAGES 75
			16. PRICE CODE
17.SECURITY CLASSIFICATION OF REPORT	18.SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

Approved for public release; distribution is unlimited.

AUTOMATED MESSAGING FOR THE GLOBAL COMMAND AND CONTROL SYSTEM: ANALYSIS OF UPGRADING COMMUNICATIONS IN THE NPS SECURE SYSTEMS TECHNOLOGY LABORATORY (SSTL)

Shenae Y. Morrow
Lieutenant, United States Navy
B.S., Colorado State University, 1987

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1996

ABSTRACT

The Global Command and Control System (GCCS) is currently operational in the Secure Systems Technology Laboratory located in Root Hall at the Naval Postgraduate School. All subsystems of GCCS are operational with the exception of the Automated Message Handling System (AMHS). The SSTL's efforts to obtain an operational GCCS AMHS depends on the future availability of the Automated Defense Information Network (AUTODIN), and the emerging technology of the Defense Message System (DMS). This thesis examines and compares GCCS AMHS and DMS and the implementation requirements for each. This thesis draws the conclusion that DMS is the dominant system over GCCS AMHS and continues to examine the acquisition strategies and costs required to implement the DMS in the SSTL.

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

ADUA	Administrative Directory User Agent
AMHS	Automated Message Handling System
AMPE	Automated Message Processing Exchange
ASC	AUTODIN Switching Center
ASCII	American Standard Code for Information Exchange
AUTODIN	Automatic Digital Network
BLII	Base-Level Information Infrastructure
CAP	Component Approval Process
CAW	Certification Authority Workstation
CCITT	International Telegraph and Telephone Consultative Committee
CCPII	Communications Control Processor II
CINC	Commander-In-Chief
CIS	Computer Information System
CMM	Classified Materials Manager
CNET	Chief of Naval Education and Training
COE	Common Operating Environment
COP	Common Operating Picture
COTS	Commercial Off-the-Shelf
CSP	Communications Support Processor
C2	Command and Control
C3I	Command, Control, Communications and Intelligence
C4I	Command, Control, Communications, Computers and Intelligence
C4IFTW	C4I for the Warrior
DAC	Discretionary Access Control
DD173	Specific Joint Message Format
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMA	Defense Mapping Agency
DMS	Defense Message System
DoD	Department of Defense
DoN	Department of the Navy
DSA	Directory Service Agent
DUA	Directory User Agent
EC/EDI	Electronic Commerce/Electronic Data Interchange
E-MAIL	Electronic Mail
GB	Gigabyte
GCC	Global Control Center
GCCS	Global Command and Control Center
GENSER	General Services

GOTS	Government Off-the-Shelf
GSORTS	Global Status Of Resources and Training System
GUI	Graphic User Interface
IDIQ	Indefinite delivery/Indefininte quantity
IOC	Initial Operating Capability
IOT&E	Initial Operational Test and Evaluation
JANAP	Joint Army, Navy, Air Force Publication
JCS	Joint Chiefs of Staff
JDIS	Joint Defense Intelligence Service
JMCIS	Joint Maritime Command Information System
JOPES	Joint Operations Planning and Execution Systems
JPL	Jet Propulsion Laboratory
JWICS	Joint Worldwide Intelligence Communication System
LAN	Local Area Network
LCC	Local Control Center
MB	Megabyte
MDS	Message Dissemination Subsystem
MFI	Multi-Function Interpreter
MISSI	Multi-level Information System Security Initiative
MLA	Mail List Agent
MLS	Multi-level Secure
MM	Message Manager for AMHS; Military Message for DMS
MROC	Multi-command Required Operational Capability
MS	Message Store
MS DOS	MicroSoft Disk Operating System
MTA	Message Transfer Agent
MTF	Message Text Format
MTS	Message Transfer System
MWS	Management Workstation
NATO	North Atlantic Treaty Organization
NASA	National Aeronautics and Space Administration
NCTC	Naval Computer and Telecommunications Command
NIC	Network Interface Card
NIPRNET	Unclassified-but-Sensitive Internet Protocol Router Network
NPS	Naval Postgraduate School
NSA	National Security Administraion
NTCC	Naval Telecommunications Center
NCTAMS	Naval Computer & Telecommunications Area Master Station
O&M	Operations and Maintenance
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
PLA	Plain Language Address

PMO	Program Management Office
POM	Program Objective Memorandum
PUA	Profiling User Agent
RAM	Random Access Memory
RCC	Regional Control Center
RI	Routing Indicator
SA	Systems Administrator
SAT/CBT	Standard Automated Terminal/CSP Backside Terminal
SBU	Sensitive but Unclassified
SCIF	Secure Compartmented Information Facility
SIPRNET	Secret Internet Protocol Router Network
SNS	Secure Network Server
SPAWAR	Space and Naval Warfare Systems Command
SSTL	Secure Systems Technology Laboratory
STU-III	Secure Telephone Unit
TCP/IP	Transport Control Protocol/ Internet Protocol
UA	User Agent
WAN	Wide Area Network
WWMCCS	World Wide Military Command and Control System
WWW	World Wide Web

I. INTRODUCTION

For over thirty years, the standard element in organizational messaging DoD wide has been the Automated Digital Network (AUTODIN).[1] AUTODIN supports Multi-level Security (MLS); in other words, it supports all levels of message security classifications. Although AUTODIN is a trusted communication system (i.e., it is secure), the overhead required to maintain and operate the system and its aging mainframe technology make the system expensive and slow.

In the late 1980's and early 1990's, computer based technological developments made it possible to modify or replace AUTODIN messaging. Some of the developments use PC/UNIX based software and the AUTODIN backbone and to automate inbound and outbound message processing, while other systems are used for inbound message dissemination only. Still, another technology once fully implemented would not use AUTODIN at all. These new systems will be discussed later in this thesis. The remainder of this chapter presents the statement of the thesis problem, the purpose and scope of this research, and outlines the organization of this study.

A. PROBLEM STATEMENT

The Secure Systems Technology Laboratory (SSTL) is located in Root Hall at the Naval Postgraduate School (NPS). In December 1995, the Global Command and Control System (GCCS) was installed in the SSTL to provide NPS students and other users (e.g. Reserve units) real-time warfighting experience. The GCCS installed in the SSTL is the same GCCS installed at CINC sites and could serve as an alternate or additional operational CINC site. The NPS GCCS site will also be used by students to participate in CINC level exercises (eg., to role play non-participating

---

[1]AUTODIN is a worldwide, computerized general purpose communications system based on mainframe technology. It provides for the transmission of both narrative and data pattern official organizational messages on a store-and-forward basis.

commands or to act as observers/evaluators for the CINC). Additionally, selected reserve components use the NPS GCCS site to conduct operational training prior to supplementing GCCS equipped CINC command centers.

GCCS is comprised of several subsystems to support the Command, Control, Communications, Computers, and Intelligence for the Warrior (C4IFTW) concept. All of the subsystems installed on the SSTL's GCCS are operational with the exception of its Automated Message Handling System (AMHS). GCCS AMHS is designed to automatically send and receive UNCLASSIFIED to SECRET organizational messages (using the AUTODIN backbone). The SSTL has a requirement to receive high precedence, classified organizational messages, therfore it needs to implement an operational automated messaging system for the installed GCCS.

B. PURPOSE OF RESEARCH

This thesis is conducted to examine the most viable message handling technologies available to support the SSTL's GCCS.

C. DISCUSSION

Emerging information technologies of the 1990's have spawned several significant events that have an impact on the type of messaging capability to be chosen for the SSTL's GCCS. These events are not all Navy or NPS unique thus all DoD services and agencies have similar experiences. The events are as follows:

1. The closure of NTCC Monterey in 1993 eliminated direct NPS AUTODIN access.
2. Assistant Secretary of Defense (C3I) 9 March 1995 mandated closure of AUTODIN by year 2000 is changing the methods in which the DoD must handle its message traffic [Ref. 14].
3. The Development of the Defense Information Infrastructure (DII) has highlighted the need for DoD communications systems to become more integrated.
4. The DOD's transition to the Defense Message System will lessen the reliance on AUTODIN as a messaging system.

These problematic events are discussed in greater detail later in the thesis.

D. SCOPE

This thesis is limited in scope to the requirements and information needed to provide the SSTL's GCCS with a viable automated message handling system. Specific communication systems, methods, and policy at the DISA, DoN, and NPS level will be discussed to provide clarity, understanding, and examine interoperability issues. GCCS AMHS and DMS are discussed and compared in-depth to the DoD's messaging requirements, however, the chapters that follow examine and compare only the messaging technology deemed best for the SSTL.

E. ORGANIZATION OF THE STUDY

The study's chapters present the following information:

- Chapter I introduces the problem, purpose and scope.
- Chapter II is a communication systems overview of GCCS, GCCS AMHS and DMS.
- Chapter III introduces the current procedures by which NPS receives external message traffic.
- Chapter IV examines the specific hardware and software requirements of the GCCS Automated Message Handling System.
- Chapter V examines the specific hardware and software requirements of the Defense Message System.
- Chapter VI provides a functional comparison of GCCS AMHS and DMS.
- Chapter VII discusses DMS acquisition and procurement costs for the SSTL.
- Chapter VIII discusses the conclusions reached as a result of the study.
- Chapter IX contains recommendations for further areas of study and closing remarks.

II. COMMUNICATION SYSTEMS REVIEW

This chapter provides a general discussion of GCCS, GCCS AMHS, and DMS to lay a foundation for comparison and selection of the best messaging system for the SSTL.

A. GLOBAL COMMAND AND CONTROL SYSTEM (GCCS)

The GCCS is a family of applications built to achieve two main objectives: (1) to replace the aging mainframe based Worldwide Military Command and Control System (WWMCCS) and (2) to begin implementation of C4I for the Warrior (C4IFTW) concept [Ref. 1]. GCCS, when fully activated will offer the warfighter highly mobile, deployable, command and control (C2) with a fused, real-time, true representation of the battle space. The system will be a comprehensive, global system that provides warfighters with required flexible and interoperable command and control, anytime and anywhere. GCCS uses the Secret Internet Protocol Routed Network (SIPRNET) - the secret portion of the Defense Information System Network (DISN)- for intersite connectivity. This joint-service data network provides DoD with a faster, smarter central nervous system. GCCS also receives information from tactical communications systems, which are physically connected to individual GCCS nodes within the larger network of GCCS sites (i.e. mobile). GCCS passed its Initial Operational Capability (IOC) test in August 1996. In its current version it offers the warfighter much more capability than WWMCCS, but is only at the first of many steps in achieving full implementation of C4IFTW.

To gain a better understanding of GCCS, the following scenario is provided [Ref. 2]:

> A simplified GCCS command center equipped with two projection panels and 10 workstations responds to a military crisis (in the fictitious region known as the Southern Coast of California). Commanders tap into the Joint Defense Intelligence Service (JDIS)

application to get detailed information about enemy troop placements, weapon capabilities and the like.

Using the DoD INTELINKS, a graphical intelligence network interface based on the World Wide Web (WWW), commanders access operational secret level homepages to view detailed photographs of enemy tanks, recent satellite images showing their movements and thousands of other bits of intelligence pulled from DISN's SIPRNET.

Needing a near-real time tactical display, the Common Operation Picture (COP) application from the chart portion of the Joint Maritime Command Information System (JMCIS)[2] is used to display regional maps with icons representing the location of both enemy and U.S. military assets. A click on a particular icon produces a screen with detailed descriptions of units, equipment and the location of those assets. This data overlays digital maps downloaded from Defense Mapping Agency (DMA) databases.

After assessing the operational situation, an additional set of Joint Operations Planning and Execution System (JOPES) based GCCS applications help commanders develop courses of action. For example, the use of Global Status Of Resources and Training System (GSORTS) indicates which U.S. troops and weapons are ready for deployment, while the Scheduling and Movement (S&M) System determines the best way of getting units to the theater of war on time. Numerous messages are sent up and down the chain of command using the GCCS AMHS for organizational messages and the GCCS E-mail application for individual messages.

Future GCCS applications, such as the Logistics Anchor Desk and the Medical Anchor Desk, will serve as funnels for coordinating more detailed activities with thousands of offices and units in the field.

GCCS is the first system to use a DoD mandated joint Common Operating Environment (COE).[3] GCCS integration emphasizes the use of commercial-off-the-shelf (COTS) products and merges the capabilities of a Local Area Network (LAN),

---

[2]JMCIS currently typically provides near real-time location of Naval Units.

[3]Common Operating Environment refers to a core group of software functions shared by multiple applications

UNIX-based client/server architecture, desktop-style Graphical User Interface (GUI), and Relational Data Base Management Systems (DBMS) [Ref. 3].

The GCCS client/server architecture provides a foundation for linking external systems and GCCS components, permitting easy access to applications, and faster, more reliable data transfers within a secure environment.

At the core of GCCS are large databases and application servers connected to a secret LAN. The GCCS LAN interconnects GCCS servers with a variety of client workstations such as PC DOS, MicroSoft windows for PCs, Macintosh, UNIX and other X Windows clients, that run server-based software and application packages. The GCCS LAN also connects with secret Wide Area Networks (WANs) supporting standard LAN design (currently the SIPRNET).

B. GCCS AUTOMATED MESSAGE HANDLING SYSTEM (AMHS)

Since the early 1990's, a variety of Automated Message Handling Systems (AMHS) have been used to automate and enhance traditional methods of sending, receiving, and storing official AUTODIN messages at different security levels within the DoD. AUTODIN is the baseline messaging environment of DoD and its processes will be discussed in greater detail in Chapter III.

One application of AMHS, specifically the one used by EUCOM, was chosen under the GCCS Best of Breed concept to be the basis for the GCCS AMHS.[4] This AMHS is integrated into the GCCS COE with several other COE functions as shown in Figure 2.1.

---

[4]GCCS AMHS installed in the SSTL processes UNCLASSIFIED TO SECRET messages. It was developed by the National Aeronautics and Space Administration's (NASA) Jet Propulsion Laboratory (JPL) for GCCS.

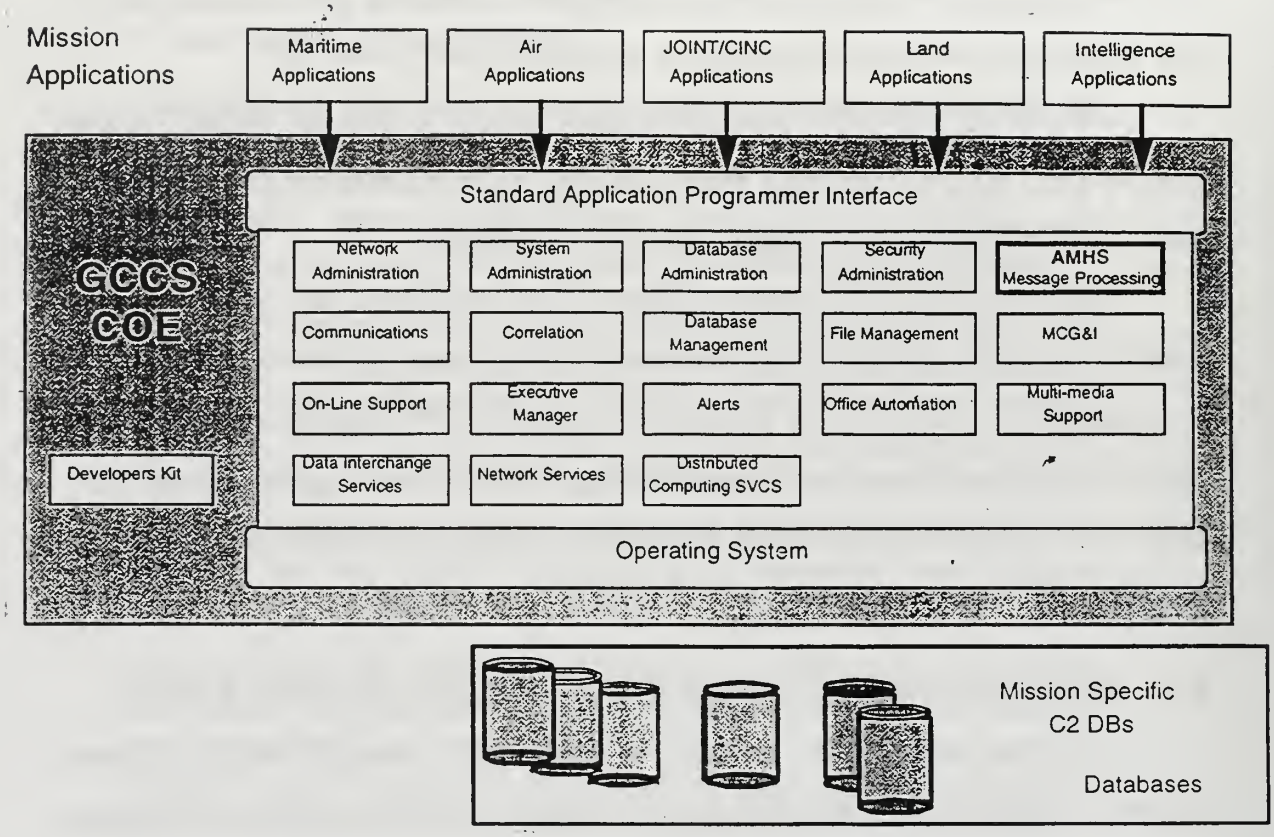

Figure 2.1. GCCS Common Operating Environment

GCCS AMHS is a front end system to AUTODIN and as such, requires an AUTODIN feed directly to the user's command.

As an extension of AUTODIN, GCCS AMHS uses knowledge based tools and COTS products to accelerate message handling processes and procedures. GCCS AMHS provides three basic functions [Ref. 4]:

(1) Automated receipt, storage, and distribution to the user of AUTODIN messages.

(2) Retrospective search and recall of stored messages (60 days, configurable).

(3) Support for generating, verifying, approving and transmitting AUTODIN messages.

C. DEFENSE MESSAGE SYSTEM (DMS)

DMS consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in the DoD. DMS is designed to provide organizational message and electronic mail (E-mail) service to all DoD users and access to and from worldwide DoD locations. It will also provide interfaces to other US Government, allied, tactical, and Defense contractor users as needed. This will be achieved by compliance with X.400/X.500 international standards for digitally switched messages.[5] DMS is based upon the principles of standardization and interoperability with other DISA systems such as GCCS (Figure 2.2).

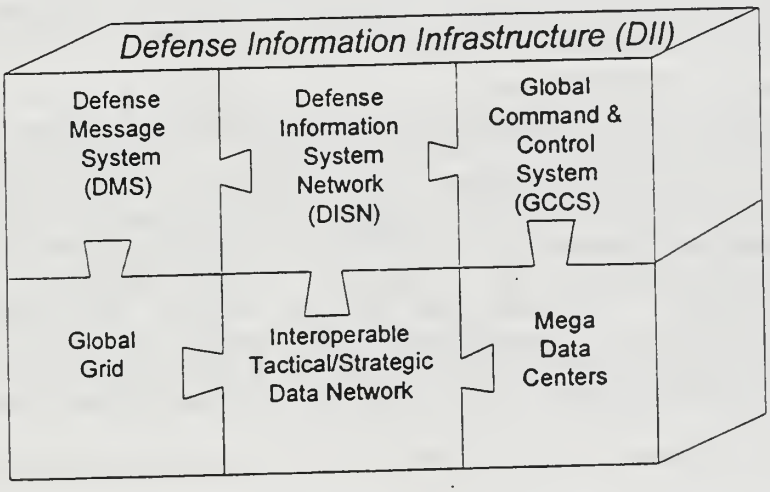

Figure 2.2. DISA's Interoperability

DMS' objectives are to meet DoD requirements for secure, accountable, and reliable, writer-to-reader message services at all classification levels (unclassified to

---

[5]X.400 and X.500 are international standard protocols developed by the International Telegraph and Telephone Consultative Committee (CTTII). X.400 provides a store-and-forward message handling system in a multi-vendor environment. X.500 provides for directory services for electronic mail.

TOP SECRET/SCI), to the warfighter as a replacement for and improvement over AUTODIN. All components of DMS will consist of readily available COTS products. In its transition stages, DMS will interoperate with current message systems (such as AUTODIN) as they evolve from current configurations to full implementation. Basic functions of DMS include [Ref. 5]:

(1) Secure support for automated receipt, storage and distribution of DMS messages at all classification levels.

(2) Secure support for generating, verifying, approving and transmitting DMS messages.

(3) The ability to provide a single capability to the end user (writer/reader) for organizational (official) and individual (E-mail) messaging.

(4) Secure support for directory services to ensure messages are properly addressed and reach the correct destination.

During the DMS implementation period, classified local systems like GCCS will maintain their required connectivity via the SIPRNET, and unclassified local systems will maintain their connectivity via NIPRNET through appropriate filters in their individual firewalls. As more local systems become DMS equipped, the AUTODIN system and the use of the SIPRNET will be fully merged into DISN [Ref. 6].

D. MESSAGE HANDLING FUNCTIONALITY

DMS is an improvement over AUTODIN-based systems. Not only does its protocol allow for more efficient transmission of data, voice, video and multi-media products, but also provides the functionality of an AMHS. Specific functional characteristics of AMHS and DMS and their integration with GCCS will be discussed in Chapter VI.

III. CURRENT MESSAGE SERVICE

In this chapter, the discussion provides a historical perspective of communications systems and discusses systems that are currently in use by the Naval Postgraduate School (NPS) and requirements for the Secure Systems Technology Laboratory (SSTL).

A. HISTORICAL BACKGROUND

The standard element in organizational messaging across the DoD is the Automated Digital Network (AUTODIN). Since the 1960's, the Department of the Navy has used AUTODIN as the backbone for delivery of organizational General Service (GENSER) Messages. AUTODIN Switching Centers (ASC's), are main "connectors" in the AUTODIN system that route GENSER messages from other ASC's within a designated geographical area. Baseline AUTODIN included 15 operational ASCs located throughout the continental U.S. and overseas [Ref. 7]. Once the message leaves the ASC it is routed to an Automated Message Processing Exchange (AMPE) or a Naval Telecommunications Center (NTCC). An AMPE serves as an extension of an ASC. AMPEs provide limited switching functions in the same manner of an ASC as well as conversions of destination Plain Language Addresses (PLA) into internal AUTODIN addresses (routing indicators) and distribution determination of messages. An NTCC, is the interface for entry and exit of messages to and from AUTODIN for organizations located in its geographical vicinity. NTCCs provide over-the-counter message service (sending and receiving) to its assigned organizations. AUTODIN messages received by an NTCC are duplicated and distributed on paper or floppy disks (since 1990 paper has been gradually replaced by disks as the preferred medium). A courier from an organization must physically pick up copies of incoming messages or drop off outgoing messages

at the NTCC. In recent years, many NTCCs have closed in favor of AUTODIN message service using the GateGuard system described in the next section.

B. MESSAGE SERVICE AT NPS

Since the closing of NTCC Monterey in 1993, GENSER messages at NPS are delivered and sent via GateGuard.[6]

GateGuard is the first DoN message system to fulfill the objective of electronically extending messaging services to the user level [Ref. 8]. GateGuard is a program installed on a PC that serves as an AUTODIN interface point for NPS. GateGuard is approved to process Unclassified-but-Sensitive through TOP SECRET messages. The system at NPS processes messages through SECRET. NPS messages received at NTCC Oakland are transferred electronically (downloaded) by the NPS Classified Message Manager (CMM) to the GateGuard using a STU-III phone. Incoming unclassified messages are taken off the GateGuard PC and moved onto a second PC installed with the Message Dissemination Subsystem (MDS) program. The MDS PC is connected to the NPS LAN and distributes these incoming unclassified messages to the designated department or individual [Ref. 9]. Classified messages are moved from the GateGuard PC onto disk. A courier from the Sensitive Compartmented Information Facility (SCIF) picks up the disk, takes it to the SCIF and prints the messages from the disk. A SCIF staff member cleanses the disk and the courier delivers the disk and hard copies of the classified messages to the CMM. The CMM then notifies the message recipient for pick-up.

Outgoing unclassified messages are delivered to the NPS CMM by courier. Outgoing messages are given to the CMM on disk with an accompanying paper copy of the message containing the releasing authority's signature. The CMM sends the

---

[6]GateGuard is a DMS transitional system that enabled the closing of NTCC Monterey.

message through GateGuard via STU-III to Oakland NTCC to be release to AUTODIN. Outgoing classified messages are drafted on a classified PC using a Message Text Format Editor (MTF). The disk and hard copy (with releasing authority's signature) are hand carried to the Classified Materials vault for release via GateGuard [Ref. 9].

C. MESSAGE SERVICE FOR THE SSTL

AUTODIN Message Service in the SSTL is currently non-existent. However, up to Secret Level E-mail to SIPRNET users is available. The SSTL is not connected to the NPS LAN therefore, it does not receive unclassified messages using the MDS program. Any classified messages received for the SSTL must be picked up by courier from Classified Materials vault.

IV. AMHS REQUIREMENTS FOR THE SSTL

This chapter examines the specific software and hardware requirements for the SSTL to operate a functional GCCS AMHS using AUTODIN lines. GCCS AMHS is a functional system at various GCCS sites world wide, therefore the discussion in this chapter written in present tense. The GCCS AMHS Administration Manual for Solaris [Ref. 4] was used as the basis for this chapter.

A. GENERAL BACKGROUND

Before a message arrives at the SSTL, it must be transmitted through AUTODIN (Figure 4.1). The GCCS AMHS infrastructure begins at the physical point where the AUTODIN feed stops. The feed connects directly into the GCCS Data Center where the AMHS architecture then takes over. Figure 4.2 is a block diagram of this process.

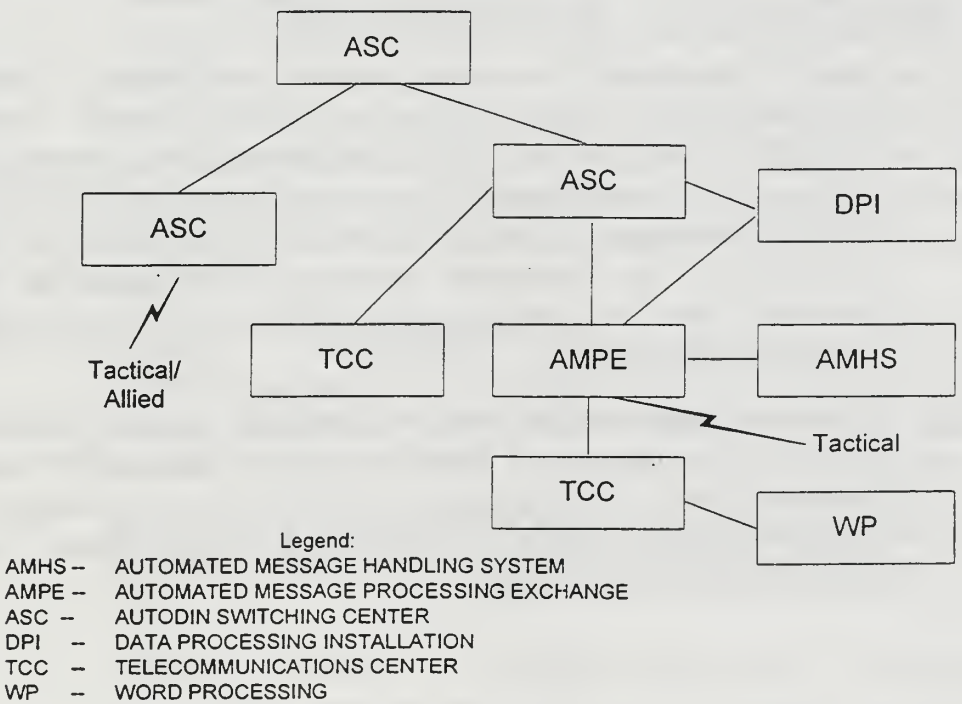

Figure 4.1. Automated Digital Network (AUTODIN)

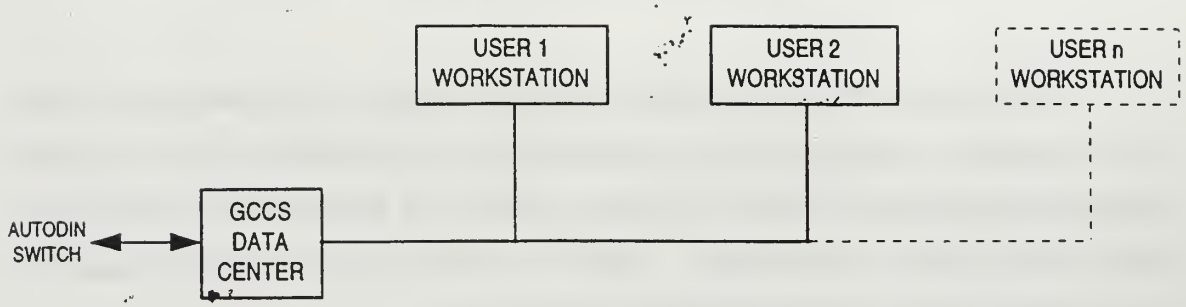

Figure 4.2. AMHS Functional Block Diagram

The GCCS AMHS architecture is designed to fit the size of the site in which it is to be installed. The SSTL, considered a small site due to its anticipated low AUTODIN traffic load,[7] requires a single server, that can support all or some GCCS COE components and applications, including GCCS AMHS.

In Chapter II, Part B, the basic functions of GCCS AMHS were described. These same functions can now be described in terms of the specific hardware and software required for the SSTL. The AMHS GCCS [Ref. 7]:

(1) Accepts messages via the Standard Automated Terminal/ Communications Support Processor (CSP) Backside Terminal (SAT/CBT) from the AUTODIN Switching Center, decrypts the messages, and stores them in file system drive on the GCCS AMHS Server. The messages are routed by the GCCS AMHS Server over the secret LAN to the appropriate recipients (when logged into client machines) based on predetermined profiles and criteria using the TOPIC software program.

(2) Assists users who author messages through the Message Text Format (MTF) Editor, then routes them for approval through the Message Manager (MM). Once approved, the MM releases messages with format validation, to the AUTODIN switch via the Releaser program of the MM and the SAT/CBT.

---

[7]Traffic load determined by Ref. [19].

(3) Searches for key words in a message database using the TOPIC retrospective search tools to locate any message that relates to user-defined criteria (this can be both address and/or content).

Specific explanations of software and hardware requirements are discussed in the next section.

B. SOFTWARE REQUIREMENTS

GCCS AMHS requires a number of software programs to assist in the message handling process.

1. COTS Verity TOPIC is used as the GCCS AMHS text profiler and retrieval database engine. It provides access to incoming AUTODIN messages, notification to the message writer that the message has been released (called come back copies) and coordination traffic. As messages are received, they are put into the message database based on discretionary access control (DAC) filters. Upon message queue delivery, users can query the database using the TOPIC Query Manager.

2. Message Manager (MM) provides the capability to create or retrieve a message, modify the textual content of the message, and transmit that message to one or more users within the LAN. MM may accept a transferred message, provide a response generation window for the user to input response message text, and transfer the response to the initiator of the original message. Database storage for message storage and retrieval, and review coordination in support of message export are also provided.

3. Message Text Format (MTF) Editor supports the creation of fully formatted messages for transmission onto AUTODIN (i.e. outbound message processing). Pre-designed message templates have been incorporated, making it easy for the user to generate messages.

4. AMHS Server version 5.01 is support software for the TOPIC server (located on the AMHS server). This must be installed on the server only.

5. AMHS Client version 5.01 is support software for TOPIC interaction by the client workstation(s). It must be installed on the system administrators client workstation and should be installed an all other client (user) workstations that use GCCS AMHS.

6. AMHS Release Patches are software updates supplied by DISA which include installation and operation notes detailing the changes and how they affect system operation.

7. SAT/CBT software accepts and releases messages from the AUTODIN Switching Center.

C. HARDWARE REQUIREMENTS FOR THE SSTL

The hardware requirements to operate GCCS AMHS in the SSTL are based on the small site configuration. Except for the AUTODIN feed, the SSTL has the required hardware onboard.

1. Sun Sparc20 or above running Solaris 2.3 - to serve as the AMHS server, TOPIC Database Server.

2. Sun Sparc20 or above running Solaris 2.3 - to serve as a client workstation for the Systems Administrator. A user workstation can serve as this function.

3. 2 GB Hard Disk Space - to support up to 60 days archive and 1000 messages per day.

4. PC-386 or better (using MS DOS) to serve as the Standard Automated Terminal/ Communications Support Processor Backside Terminal (SAT/CBT).

5. CCPII AUTODIN interface card. This card, developed by Cavalier Communications Inc., is installed in the SAT/CBT to perform the necessary cryptology functions as the messages transition to and from AUTODIN.

6. AUTODIN Feed capable of transferring 4800 bits per second.

The SSTL does not have the AUTODIN Feed, a designated dedicated PC, or the CCPII AUTODIN interface card.

D. TECHNICAL SUPPORT

Technical assistance for AMHS can be obtained from a number of sources. The Jet Propulsion Laboratory (JPL) updates its AMHS documentation and forwards

the information to all GCCS AMHS sites. DISA provides technical phone assistance through its GCCS/AMHS division. The SSTL currently has access to these resources.

E. TRAINING

User and Administrator training is available through the 81st Training Group, 333rd Training Squadron at Keesler Air Force Base, Mississippi. The 333rd Training Squadron conducts on-site training upon request. The command also developed the GCCS AMHS Study Guide and Workbook [Ref. 10] which it disseminates to its customers and is available in the SSTL. The SSTL currently has access to these resources.

F. PERSONNEL REQUIREMENTS

Ideally, a dedicated AMHS Systems Administrator should be assigned to handle the daily operations, maintenance, and manual requirements of the system. In the case of the SSTL, the GCCS systems administrator can serve as the AMHS systems administrator due to the anticipated low volume of message traffic.[8]

---

[8]The SSTL currently has only one person who serves as GCCS manager, System Administrator, Security Officer and other functions. Installation of an AMHS in the SSTL may not be feasible until additional SSTL Personnel are in place.

V. DMS REQUIREMENTS FOR THE SSTL

The specific software and hardware requirements for the SSTL to implement DMS will be examined in this chapter. DMS is going through its final testing stages therefore, the discussion that follows is written in future tense. The target date for the first DoN operational DMS site is January 1997 with a DoN wide operational implementation date of 1 January 2000. NPS is scheduled to have DMS operational by January 1999. [Ref. 6]

A. GENERAL BACKGROUND

Messages that arrive over TCP/IP via the NIPRNET at the SSTL will be transmitted through the DMS infrastructure using X.400/X.500 protocols. DISA will be responsible for installing, funding, and maintaining the main infrastructure of DMS. The target infrastructure consists of the following components which are shown in Figure 5.1 and discussed in the following sections [Ref. 5]:

1. Message Transfer Agent (MTA): The MTA is an independent store and forward message switch that will be responsible for handling the routing and transferring of messages (referred to as "envelopes"). The MTA will perform basic functions such as message receipt from a User Agent (UA), Message Store (MS), or another MTA. The collection of interconnected MTAs is referred to as the Message Transfer System (MTS).

2. Message Store (MS): The MS is collocated with the local MTA. The MS will receive and store messages when the UA is not available. The MS can be configured to alert its UA when a message of a specified type is received, and automatically forward it according to the recipient's instructions.

3. Directory System Agent (DSA): the DSA will respond to queries for directory information from Directory User Agents (DUA).

4. Mail List Agent (MLA): The MLA will support the distribution of messages through the use of common mailing lists. MLAs will be implemented locally and regionally (e.g., one MLA to serve the entire European Theater.

5. Multi-function Interpreter (MFI): The MFI is a transitional component that will allow the MTS to exchange messages with users of legacy messaging systems (e.g. AUTODIN).

6. Certification Authority Workstation (CAW): The PC-based CAW will be used to program and maintain Fortezza Cards for users.

7. Secure Network Server (SNS): The SNS high-assurance guard will control the exchange of messages to ensure that Classified information does not leap beyond the walls of a high security network.

8. Administrative Directory User Agent (ADUA): The ADUA software application will provide the directory administrator the ability to modify, add, and delete DMS directory information.

9. Management Workstation (MWS): MWS is a software application that will provide remote monitoring and control of all DMS products. It will gather DMS system information globally. The MWS should be implemented on a high performance UNIX or NT workstation.

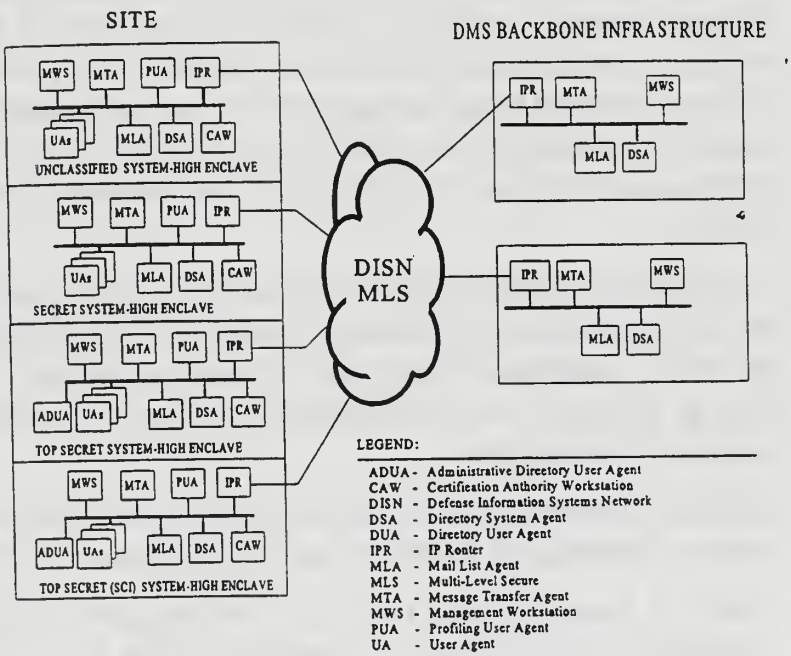

Figure 5.1. Representation of the DMS Goal Architecture

Once the message transits through DISA's DMS infrastructure, it will arrive at the SSTL. Specific hardware and software required in the SSTL to process DMS organizational messages are discussed in the next section.

B. DMS SOFTWARE REQUIREMENTS

At the organizational and individual user level, the following software is required for DMS:

1. User Agent (UA): The UA application will reside on a PC or workstation to provide the interface between the an individual user and the MTS. The UA interacts directly with the user through a GUI to create and edit a message. It will receive and display incoming message content and assist the user in replying, forwarding, filing and retrieving messages. The UA will interact with the MTA to perform security validation in order to prevent unauthorized UA's from accessing the MTS.

2. Directory User Agent (DUA): The DUA will provide directory services for organizational and individual messages. Additionally, the DUA will provide user authentication and local caching of directory information. All directory services will be provided to DMS users and components (e.g. UA, MLA, and MFI) through DUAs.

3. Profiling User Agent (PUA): The PUA is an enhanced UA that will have the primary purpose of receiving messages from an MTA on behalf of organizational users. The original message will be both delivered to and received by the PUA. Once the PUA determines the appropriate recipients to receive the message, it will resubmit copies of the message to the MTS for subsequent delivery. The PUA will redistribute the messages based on key words or phrases in the subject, priority, or message content.

The UA and DUA will be installed at the SSTL and NPS level while the PUA is an NPS only level component.

C. HARDWARE REQUIREMENTS FOR THE SSTL

1. Workstations/PCs: UNIX-based workstations or PC 486-66 SX or DX (or higher) to house the DMS software applications. DMS components can be installed on all or selected PCs or workstations [Ref. 5].

2. 16 MB RAM, 500 MB hard drive: This is the minimum requirement for DMS software recommended by the DoN DMS Program Management Office (PMO). Other applications (word processing, spreadsheets, etc.) currently installed on a PC must be considered when determining RAM and hard drive capacity.

3. Dual slot Type II Personal Computer Memory Card International Association (PCMCIA) card reader: The PCMCIA card reader will be installed on all DMS workstations/PCs to read the Fortezza security cards (explained below).

4. Fortezza Card: The Fortezza card is a cryptographic plug-in card that will provide authentication of a DMS user's identity and access privileges. The credit card sized Fortezza card, which contains its own processor and memory, will be used in conjunction with a personal identification number (PIN). Current plans are for DISA to provide all DMS users with Fortezza cards.

D. TECHNICAL SUPPORT

The DMS Program Management Office (PMO) operates under the Space and Naval Warfare Systems Command (SPAWAR 152). The DMS PMO's Infrastructure Division will provide technical support for all Navy activities and commands. Vendors will also provide software assistance as needed. NPS technical support is in the planning stages under the direction of the Computer Information Systems Department [Ref. 11].

E. TRAINING

DMS training curriculum and requirements are being developed through a DMS contractor under the guidance of DISA. Part of DISA's training mission is to provide flexibility that will allow individual commands and services to tailor training requirements to meet their specific needs. There are many options available to SSTL DMS users. The current training plan offered by DISA consists of video self-teaching and on-line help facilities. A Basic User Training course developed by DISA will also be available at designated Chief of Naval Education and Training (CNET)

training facilities or on site by mobile training teams [Ref. 7]. Detailed DoN training will be included in the DoN DMS Training Plan which will be published at a later date [Ref. 6].

F. PERSONNEL REQUIREMENTS

At the installation site level, staff will be selected to support operations, maintenance, administration, security administration, functional messaging application administration, and user assistance [Ref. 5]. This staff will come from NPS as an organization rather than SSTL designated staff. However, due to the unique nature of the GCCS system in the SSTL and its interface with DMS, the SSTL systems administrator should be considered part of the NPS support staff and receive appropriate training [Ref. 13].

VI. FUNCTIONAL COMPARISON OF MESSAGING TECHNOLOGIES

The preceding chapters of this study have served as an introduction to current and emerging communication technologies. In this chapter, AMHS and DMS functionalities are compared to the DoD's formal requirements for message communication.

A. BACKGROUND

In 1988, the Department of Defense outlined formal requirements and guidelines to develop a message communications system that is responsive to mission requirements and offered at reduced cost to the Services and Defense agencies. These requirements were defined in a joint service and agency forum and detailed in the Multi-command Required Operational Capability (MROC 3-88) [Ref. 14]. In this chapter, GCCS AMHS and DMS are compared based on the requirements and guidelines outlined in MROC 3-88.

1. MROC 3-88 Requirements

During the development of the MROC 3-88, no specific system was named. The new system, based on MROC 388 requirements, must be centered around the principles of standardization and interoperability, while preserving adaptability for implementing service and agency unique functionality and customization. [Ref. 15]

(1) Connectivity/Interoperability - Allows the user to communicate with any other user within the DoD community as well as other federal agencies, allies, tactical, and defense contractors. System users may be fixed, mobile, or transportable.

(2) Guaranteed Delivery/ Accountability - Deliver to the intended recipient with a high degree of certainty. Provide prompt notification of non-delivery to sender. Maintain writer to reader accountability.

(3) Timely delivery - Recognize messages that require preferential handling subject to traffic loads, conditions, and precedence.

(4) Confidentiality/ Security - Preclude access to or release of information to unauthorized recipients according to their security level and sensitivity.

(5) Sender authentication - Verify that information marked as originating at a given source actually originated there. Verify message is approved by competent authority before transmission.

(6) Integrity - Ensure information received is the same as information sent.

(7) Survivability - The system does not degrade the survivability of systems interfaced to it.

(8) Availability/Reliability - Provide users with continuous message service achieved by a combination of highly reliable and readily maintainable components, thoroughly tested software, and necessary operational procedures.

(9) Ease of Use - The system flexibility and responsiveness should allow user operation without extensive training.

(10) Identification of Recipients - The sender can unambiguously identify the intended recipient organizations or individuals.

(11) Message Preparation Support - Support user-friendly preparation of messages for transmission.

(12) Storage and Retrieval Support - Support storing messages after delivery to allow retrieval for such purposes as readdressal, retransmission, and other functions such as archiving and analysis. The system should also have the capability of incorporating segments into future messages.

(13) Distribution Determination and Delivery - Determine the destination of each message and effect delivery in accordance with the requirements of the recipient organization.

B. COMPARISON TO MROC 3-88 REQUIREMENTS

Table 6.1 compares GCCS AMHS and DMS to the requirements of MROC 3-88 [Refs. 4,7,15]. Because the emphasis of this thesis is on organizational messaging, E-mail is not included in the table, but it will be discussed later in section E.1 of this chapter.

Table 6.1. MROC 3-88 Comparison

MROC 3-88 Requirements	GCCS AMHS	DMS
Connectivity/ Interoperability	User can send and receive AUTODIN messages only.	User will send DMS organizational and individual messages and receive AUTODIN messages through the MFI.
Guaranteed Delivery/ Accountability	Inbound/outbound message delivery and nondelivery must be audited by the SA who will send notification over the LAN to the sender.	Delivery/Nondelivery notification will be automated. The UA audits the log of sent messages for delivery/ nondelivery notifications.
Timely Delivery	AMHS uses a Topic tree based on Topic precedence rules to queue messages. Once the message is released, AUTODIN precedence rules apply	UA will queue a message according to precedence levels. The MTA and MFI will deliver messages to UA in accordance with precedence criteria.
Confidentiality/ Security	Messages are encrypted/decrypted in the SAT/CBT therefore, messages in the AMHS are in ASCII text (readable). Uses DAC to protect against unauthorized access. SA adds, modifies and deletes DAC groups for a user.	Messages will be encrypted by the sender and can only be decrypted by the intended recipient using the Fortezza card. Fortezza cards will contain security classification labels for users.
Sender Authentication	Messages are released to the SAT/CBT through the MM Release function by the person with releasing authority.	Messages will be released at the releasing authority's UA
Integrity	Comeback copies[9] of a successfully transmitted message are delivered to the drafter, those in the routing chain, and the releaser of the message.	MISSI services will detect unauthorized changes to a messages content.

[9]Comeback copies are "as transmitted" copies of messages released to and accepted by AUTODIN through the SAT/CBT.

Table 6.1. MROC 3-88 Comparison (cont.)

MROC 3-88 Requirements	GCCS AMHS	DMS
Survivability	AMHS depends on survivability of AUTODIN. AUTODIN uses redundant inter-switch routing (under the control of ASC operators) to survive. Survival relies on connections of selected AUTODIN terminals and AMPEs to multiple ASCs	Survivability will depend on the base level/long haul networks. Routing/rerouting between MTAs will be automated to deliver message as quickly as possible.
Availability/ Reliability	AMHS provides 24 hour, seven days a week message delivery service for AUTODIN customers. AUTODIN uses mainframe equipment and message storage redundancy to achieve reliability.	DMS is designed to provide 24 hour, seven days a week message delivery service for DMS and AUTODIN users. DMS will use redundant workstations or back-ups to achieve reliability at the infrastructure level.
Ease of Use	All software components use COTS and GOTS windows based applications. One day training for users is available. SA is available to help users.	All software components will use COTS and GOTS windows based applications. One day training and user help desk will be available.
Identification of Recipients	Users access the PLA drop-down menu to choose desired PLA. If PLA is not available in menu, the SA must update the PLA table.	DUA will provide user with correct Address. If address cannot be obtained from the users DUA, the DUA will access the DMS infrastructure to get the address.
Message Preparation Support	Uses MTF editor to assist in messages preparation .	UA applications will assist in message preparation.
Storage and Retrieval Support	Messages are stored on the AMHS server and are retrieved using Topic Query Database.	UA will store messages on the users PC or client account. The UA will also provide retrieval support for the user.
Distribution Determination and Delivery	The AMHS delivers a single message to multiple addresses specified in the originators message.	The MLA will support UAs in delivering a single message to multiple recipients. The MLA will perform the security functions for the UA.

C. DIFFERENCES BETWEEN GCCS AMHS AND DMS RELATIVE TO THE SSTL

GCCS AMHS and DMS functions provide the user with paperless, automated means to receive and send message traffic. While there are many similarities between the two systems, it is the differences that make DMS a more desirable system for the SSTL. These differences are addressed in terms of personnel support, equipment, and message format standards.

1. Personnel Support

For GCCS AMHS in the SSTL, a single person is required to perform as the systems administrator (SA) and the systems operator. DMS will eliminate most of the message handling responsibilities of the SSTL's system administrator (SA). Some of the functions will be automated and other functions will become the responsibility at the level of DMS that is transparent to the user i.e., NPS or above responsibility. Some of the more laborious functions are discussed below.

a. Directory Services

The GCCS AMHS SA is responsible for insuring the address directory that allows the user to choose recipients from the pull down menu is up-to-date. The SA must add, delete or modify addresses in the directory and, if needed or requested by a user, search for the address in the Message Address Directory (MAD).[10]

DMS address directory system updates are the responsibility of the DISA infrastructure. Addresses will be stored for X.400(DMS) in PLA format. In addition, the DUA will assist the user in an automated search for addresses by request or browse functions.

---

[10]The MAD contains organization names and associated PLAs. This ACP 117 series of publications included PLAs with assigned RI (routing indicator) listings [Ref. 7].

b. Local Security

The GCCS SA is responsible for maintaining and monitoring the DAC list. Using the DAC Manager application, the SA assigns control groups to a user based on information obtained from the Security Manager.

With DMS, the Certification Authority Workstation (CAW), a special purpose trusted workstation managed by NPS personnel, will be used for network security management functions. These functions include creating certificates that indicate a user's authorizations (individual messaging and/or organizational messaging release), precedence, classifications, and other security information.

c. Non-Recipient Message Delivery

All AUTODIN messages received in the GCCS AMHS must be delivered to a human for disposition. In some cases, non-delivery of a message could occur if the users TOPIC queries are not robust enough to ensure a legitimate destination for a message [Ref. 4]. If the SA has set up a dead letter file, the TOPIC Query's profiler feature will deliver messages not profiled to a specific user to the file. The SA must decide which user to route the message to based on local policy or the SA's judgement. The SA must also know whether or not the user is authorized to see the message, since the routing procedure does not preserve DAC controls. If a dead letter file is not set-up, then the message will be dropped, unread, into the message database.

DMS messages must also be delivered to a human for disposition. The Profiling User Agent (PUA) will act as the organization's message dissemination system. It will typically be implemented on an NPS managed workstation (along with other organizational messaging applications) designated to accept messages on behalf of the organization [Ref. 5]. The PUA will automatically examine each incoming message and determine its dissemination based on information that may be contained in the heading or body of the body of the message. Once the PUA determines the

proper recipients, it resubmits copies (based on the number of authorized profiles) of the message to the MTS. The MTS will deliver the message to the appropriate recipients. Since all DMS messages are encrypted and decrypted by a Fortezza card, the MTS can only deliver messages to authorized recipients. Any message that is undeliverable to a human will result in a notification of non-delivery to the originator.

d. Systems Monitoring and Maintenance

In addition to the tasks discussed above, the GCCS AMHS SA is responsible for monitoring system activities, maintaining numerous system files, directing backups, performing restores, and overseeing the overall AMHS operations. Additional tasks include [Ref. 7]:

1. Monitoring operations - monitors system activities, periodically monitors disk utilization and the status of the network/interface, and reconfigure file systems as needed to optimize performance.
2. Maintaining system files - generates user account reports, load tapes, maintain message archive, profile information and system performance.
3. Directing backups - determines backup requirements and initiates backups.
4. Implementing security procedures - maintains the TOPIC password file.
5. Controlling system configuration - monitors and maintains a log of all software and hardware changes to the system.
6. SAT/CBT Operation/Administration - oversees the operation and maintenance of the SAT/CBT PC and is the primary interface with the NTCC on AUTODIN traffic issues.

The DMS Management Workstation (MWS), managed by NPS will automate many of the tasks performed by the GCCS AMHS SA. The MWS is part of the DMS topology that consist of three levels of management [Ref. 1,14]:

Global - A global control center will manage the operational control, monitoring, and configuring on a system-wide basis.

Regional - Regional control centers will manage infrastructure components in the Western Hemisphere (DMS-WESTHEM), Europe (DMS-EUR), and the Pacific (DMS-PAC).

Local - Local control centers will manage components at sites chosen by a Service or agency. LCCs may manage one installation or several installations in a metropolitan area. For example, an LCC for Monterey would service NPS and tenant commands, POM and tenant commands, Coast Guard Station, and Fleet Numeric. These functions will be performed for the SSTL at a higher level of DMS architecture.

All control centers will have at least one MWS. At the LCC, the MWS will provide for the SSTL monitoring and control of local DMS components, accounting, security management, system administration, auditing, user account maintenance and customer service.

2. Equipment

As discussed in Chapters IV and V, GCCS AMHS and DMS require different equipment. For implementation in the SSTL, GCCS AMHS is installed with a server, a dedicated PC (for the SAT/CBT), the CCPII AUTODIN interface card and an AUTODIN feed. The system also requires the MM, MTF Editor, Topic, and AMHS applications and the GCCS COE.

For basic implementation in the SSTL , DMS has a smaller equipment list. DMS requires a card reader (internal or external) for each workstation/PC and Fortezza Cards for each DMS authorized user, the UA/DUA software for each workstation/PC, and the NIPRNET access.

3. Message Format Standards

The AUTODIN system provides for the transmission of three types of message format headers: (1) DD173, (2) JANAP 128, and (3)ACP 126 [Ref. 4]. The GCCS AMHS allows the user to author a message, using the MTF Editor, in any one of the three formats. The body of the messages can be drafted using either the MTF Editor

or the APPLIX text editor that is installed with GCCS. In any case, all AUTODIN messages must use ASCII text.

DMS when fully implemented will use only one message format header called Military Message. In addition, the message body may consist of ASCII text, graphics, videotext, and/or digitized voice.

D. SECURITY ISSUES

There is no question that AUTODIN is a secure system. As a Multi-level Secure (MLS) network it provides message service all security levels (from unclassified to Top Secret). The intention of DMS, in its transitional stage, is to maintain the existing level of security and, at full implementation, improve security.

Security is provided by the Multi-level Information System Security Initiative (MISSI) components which provides Information Security support for DMS. The objective of MISSI is to achieve MLS capability for automated information processing systems in phases. Phase I, Sensitive-But-Unclassified (SBU) message security, is currently available using untrusted workstations and the Fortezza Card. The SECRET message security capability (Phase II) is expected to be available after July 1997. This capability will be achieved using the Fortezza+(plus) card. The TS/SCI capability is expected to be available after July 1998. TS/SCI traffic will run on the Joint Worldwide Intelligence Communications System (JWICS) backbone [Ref. 6].

Initially, DMS will process SBU organizational messages only [Ref. 6]. System High Networks such as AUTODIN or SIPRNET will continue to process secret level information until the DMS goal architecture is achieved.

E. CONNECTIVITY ISSUES

Connectivity of all DoD communications systems has been the driving force behind the establishment DISA and its role as the DoD services and agencies information systems headquarters.

1. Electronic Mail (E-mail)

One of the MROC 3-88 requirements is connectivity of organizational and individual messaging (E-mail). In the current E-mail environment, a large command may have many E-mail systems in use which are not all compatible with one another. (e.g., the Pentagon has 49 different E-mail systems currently in use [Ref. 16].

GCCS AMHS does not provide individual E-mail through AUTODIN. However, up to SECRET individual E-mail is provide as a GCCS application of the SIPRNET.

One of the objectives of DMS is the support of individual E-mail. DMS will provide organizational *and* individual messaging using the X.400/X.500 protocols. All E-mail applications must be DMS compliant.

2. GCCS

GCCS AMHS was developed to be integrated into the GCCS COE and as such it is treated as a component of GCCS. DMS on the other hand is considered a value added service. A value added service relies on information infrastructure to provide information processing and information transport services. Value Added Services cross functional and organizational boundaries giving them the capability to interface with different communications systems like GCCS, Global Command Support System (GCSS), INTELINK, and other current and emerging DII functional applications.

3. The Defense Information Infrastructure (DII)

Currently, the DoD does not have an integrated information infrastructure. Local systems and their interconnecting networks are separated by levels of classification. GCCS and AUTODIN are pieces in the collection. The GCCS AMHS

use of the GCCS COE integrates the two systems. However, they cannot interface currently with other systems. The infrastructure is fragmented by multiple "stovepipe" systems that inhibit interoperability, fail to provide links between the battlefield and the power projection support base, and has no means of connecting to the U.S. Industrial Base.

The goal of DII is to operate as a collection of distributed heterogeneous information systems by the year 2000. Applications within the DII will range from centrally developed DoD applications implemented at central locations to base-level or end-user applications residing on the desktop or in tactical environments [Ref. 17].

Under the DII master plan, GCCS and DMS will be part of the heterogeneous system with AUTODIN and GCCS AMHS considered legacy systems and therefore are to be merged into or replaced by DII.

4. Interoperability

GCCS AMHS as an AUTODIN front end system cannot provide interoperability between U.S. allies and Federal agencies. DMS is designed to provide interoperability through the use of the Multi-Function Interpreter (MFI). In addition DMS will maintain interoperability with AUTODIN systems and its different formats until the phase-out is complete.

5. AUTODIN

AUTODIN is the backbone system for GCCS AMHS. In 1993, NTCC Monterey closed its doors. On 9 March 1995, the Assistant Secretary of Denfense (C3I) mandated the closing of AUTODIN by 31 December 1999 [Ref. 6]. These two events make it difficult, if not impossible, for the SSTL to implement a fully functional GCCS AMHS that is cost effective over time. AUTODIN capabilities on the Monterey Peninsula area have not been readily available to NPS since 1993. To attempt to establish that capability would require the IAC to justify spending money

on a system that has been ordered closed. DMS is the replacement for AUTODIN and its front end systems.

F. CONCLUSION

Comparatively, DMS is a better system than GCCS AMHS, but is not scheduled for NPS implementation until January 1999. GCCS AMHS has the advantage over DMS in that the system has been tested, it is operational in many commands, and software is installed, although not fully functional, because of lack of AUTODIN connectivity, in the SSTL. GCCS AMHS is used in the SSTL as an internal training system. Users can draft messages and route them through the AMHS but they cannot release or receive messages through AUTODIN.

Although it is still evolving, DMS is designed to accommodate legacy systems such as AUTODIN and front end systems such as GCCS AMHS. Unfortunately, DMS local level infrastructure is not scheduled for installation at NPS until December 1998 with operational capability in January 1999 [Ref. 6]. Initial DMS implementation at sites prior to July 1997[11] will require those organizations to receive SBU DMS products to send and receive unclassified messages only via the DISN. Existing AUTODIN components will continue to send and receive classified messages. The SSTL will have to wait until January 1999 when DMS is scheduled to be fully operational at NPS and has the capability to process SECRET messages [Ref. 6]. Under the circumstances, because AUTODIN installation is infeasible, the SSTL has no choice but to wait for DMS.

---

[11]Completion date of DMS SECRET IOC testing.

VII. DMS ACQUISITION STRATEGY AND PROCUREMENT COSTS FOR THE SSTL

This chapter examines the DMS acquisition strategy and possible procurement costs for the SSTL. GCCS AMHS and AUTODIN as legacy systems are not discussed. This chapter is based on a draft version of the DoN DMS Master Plan (for DMS implementation) that forecast costs out to 1999.

A. DMS ACQUISITION STRATEGY

The DMS program employs an acquisition strategy designed to influence development of COTS products while maintaining maximum competition and acquisition flexibility. Vendors are encouraged to provide COTS solutions to meet DoD's messaging, directory service, security, and service management requirements. Establishment of a separate DMS compliant testing environment will ensure COTS products satisfy DMS functional, security, performance, conformance, and interoperability requirements. The testing environment will allow any vendor to submit products for DMS compliance certification. Once certified, these products will be placed on a list of DMS certified products available for purchase by the Services and Agencies [Ref. 18]. The intention of the DMS acquisition strategy is to provide DoD Agencies maximum acquisition flexibility and cost savings resulting from competition and large quantity purchases.

The DMS primary acquisition contract type, indefinite delivery/indefinite quantity (IDIQ), allows the Services, Agencies, and DISA to procure DMS compliant products and services deemed necessary to achieve the target DMS architecture [Ref. 19].

The following section covers DMS procurement policy as it applies to DISA, the DoN, and NPS to define the roles and responsibilities each will play in the DMS Acquisition Plan.

1. DISA Policy

DISA is responsible for procuring hardware and software products (MTA, MWS, MFI, DSA, etc.) and support services necessary to engineer, integrate, plan, deploy, implement, and maintain/manage the DMS infrastructure. Hardware and software maintenance and operation of DMS infrastructure will be funded through the Defense Business Operating Fund (DBOF) through a rate structure which began in FY 1996. All infrastructure orders from the Services and Agencies will be processed through the DISA DMS Program Management Office [Ref. 19].

2. Navy Policy

The DoN DMS Program Management Office was established under the Space and Naval Warfare Systems Command (SPAWAR 152) to provide DMS planning and coordinating for the Navy and Marine Corps and resolve the implementation challenges associated with DMS. Funding requirements for procurement, engineering and installation, training, maintenance, and operation of user components at the LCC levels, are the responsibility of the Navy.

The DoN DMS PMO is responsible for centrally funding and acquiring each DoN activity's one enabling capability for organizational messaging to include products and services such as the CAW, security software and devices (Fortezza cards and card readers) a UA/DUA, and a PUA. This enabling capability will allow each activity to send and receive official messaging and E-mail through the DMS.

DoN DMS PMO policy require commands to fund their own firewalls, router, workstations, and upgrades for LAN infrastructure. DMS extension to the desktop (hardware and software) is the responsibility of each command. The decision has not been made if usage fees for DISN will be centrally funded or billed back to the command [Ref. 20].

The DON PMO will assist commands in determining DMS requirements based on the results of a User Site Survey. Once determined, the users will present their

user-based product ordering requirements to the PMO. The PMO will submit users ordering and DON infrastructure requirements to DISA and, after review, DISA will submit the order to the Air Force PMO who serves as the Central Ordering Office. The Contracting Office accepts the orders from the DMS-AF PMO and negotiates with the contractor. Figure 7.1 depicts the products and services ordering process. [Ref. 19]

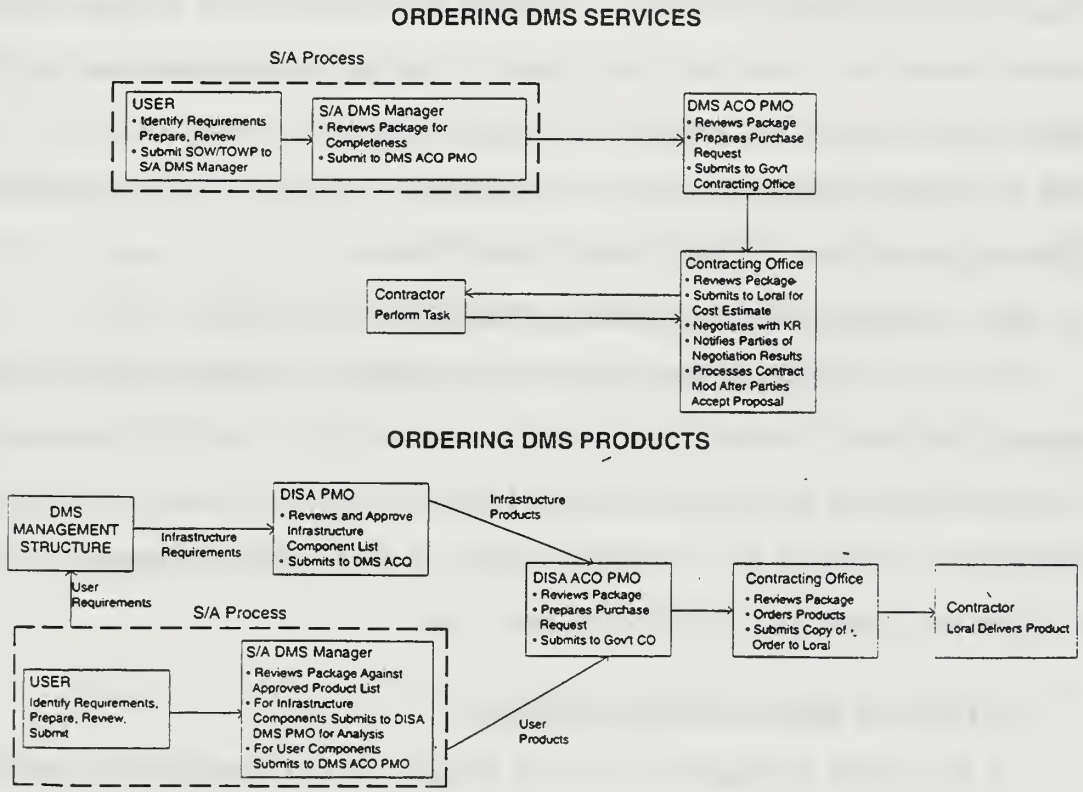

Figure 7.1. DMS Products and Services Ordering Process

An important feature of the DMS ordering system is that commands will be able to track the status of their order, through NCTAMSLANT's WWW homepage as it passes through the system.

3. NPS Policy

Commands are responsible for funding and extending messaging capabilities to individuals within their activity via their LANs. NPS, under the direction of the Assistant Provost for Computer Information Systems (Code O5) is in the process of upgrading and restructuring its LANs to make them compatible with each other [Ref. 21]. Currently, there is no complete NPS initiated DMS implementation plan [Ref. 11]. According to The DoN DMS Master Plan [Ref. 6], NPS is scheduled for its first site survey from September through December 1997 and the NPS Implementation Plan is scheduled to be completed and forwarded to the DMS PMO no later than 28 February 1998. In anticipation of DMS, part of the NPS strategy is to build the X.400/X.500 capability into the NPS wide backbone LAN [Ref. 11]. Funding at the NPS level has not been officially budgeted at this time.

4. Implications of Acquisition Policies for the SSTL

Due to the scheduled December 1998 installation of DMS at NPS, it is not surprising that there is currently no specific acquisition policy for DMS products at NPS. Until DMS site surveys are completed for NPS (the last of two site surveys is scheduled to be complete by 28 February 1998), the SSTL can only prepare to state its requirements using the DMS Draft Master Plan.

B. SSTL DMS PROCUREMENT COSTS

As the Initial Operational Test and Evaluation and Component Approval Process comes to a close, there are procurement options now available to the SSTL. The SSTL can purchase current commercial (i.e., non-DMS) versions of products either from the DMS contract or from local software outlets. Products purchased from the contract will receive vendor provided DMS upgrades for five dollars per product [Ref. 20].

It is difficult to develop a specific procurement plan and calculate life cycle cost without the benefit of a User Site Survey. The first NPS site survey, the

Engineering Field Activity (EFA)[12] survey, is scheduled for September through December 1997. The last survey (Loral product survey) is scheduled for February 1998. The procurement costs discussed in the following sections can be found in the Loral Product ordering Guide. Products and Services discussed are based on DMS requirements for the SSTL.

1. Hardware

The SSTL will use existing workstations or PCs,[13] which are connected to the SSTL's systems high LAN (SIPRNET), for its DMS model. The SSTL has 8 SunSparc workstations and 6 PCs connected to its LAN.

The SSTL's classified LAN will be electronically connected to the NPS unclassified (NIPRNET) LAN, therefore it will require installation of a high assurance guard, such as a Secure Network Server (SNS). Since the high security guard is considered part of the NPS infrastructure, the SSTL should not incur the expense of an SNS purchase. Figure 7.2 shows this connectivity.

---

[12]The EFA Implementation teams will provide technical direction at all levels of the DoN DMS such as conducting infrastructure assessments, conducting site surveys, developing plans, overseeing installation and configuration management, and conducting fielding conferences. [Ref. 6]

[13] According to MR.James Garry, NCTS San Diego, DMS Program Manager (N5), DMS is designed to operate on PCs or UNIX-based workstations [Ref. 22].

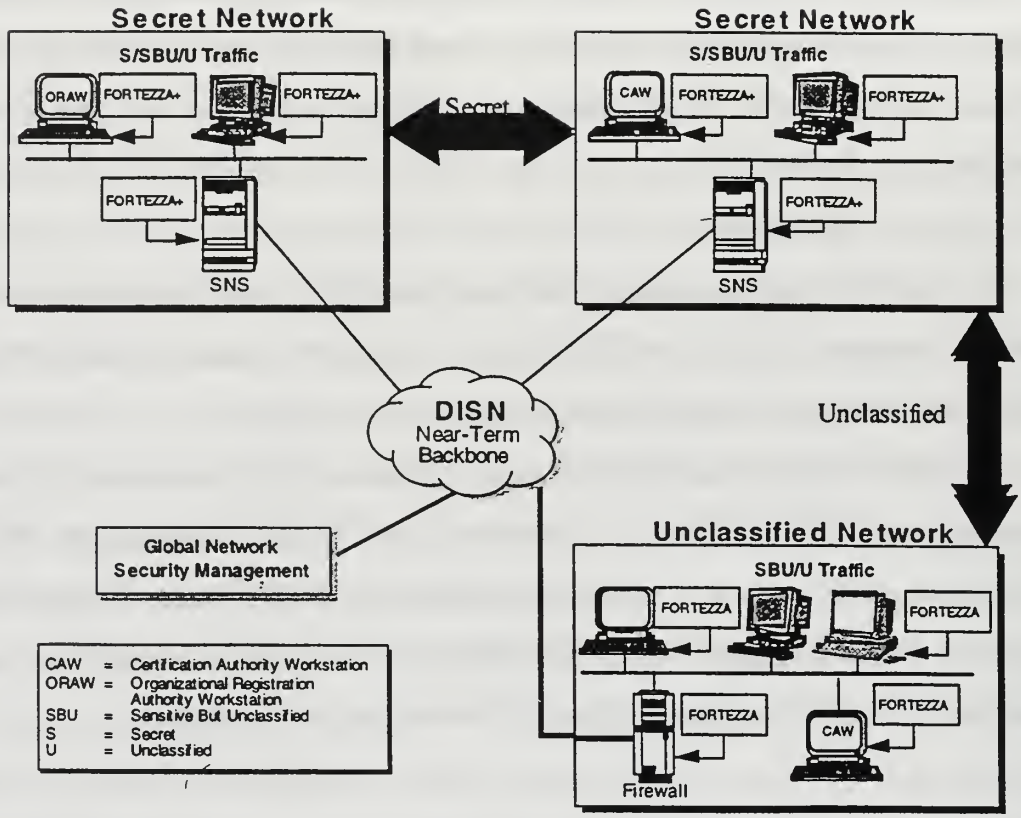

Figure 7.2. DoN DMS Security Architecture

2. Software

Commands are required to purchase any additional UA/DUAs[14] required to bring DMS to the desktop.

(a) If NPS purchases all UA/DUAs then there will be no cost to the SSTL the additional software.

(b) If the SSTL is responsible for purchasing the additional UA/DUAs for each workstation then the cost would be as follows [Ref. 19]:

UA/DUA for UNIX:	product# UA004 ESL $44 each X 8 =	$352
UA/DUA for Windows:	product# UA002 ESL $44 each X 6 =	$284
		$636

[14]The UA and DUA is combined into one software package and will be sold as such.

3. Maintenance

DMS component maintenance will be centrally funded. Network funding is the responsibility of NPS in accordance with the pending NPS DMS policy.

4. Training

Initially, training will be centrally funded by the DoN. Eventually, user training will be conducted by LCC staff. In chapter V it was mentioned that the GCCS SA should receive training beyond the user level for DMS. The DMS Orientation course will provide the GCCS SA with an overview of the DMS program, its objectives and its technology to NPS designated staff. This particular course is part of the DMS Fielding Conference which is scheduled for NPS in January 1998. [Ref. 6]

5. Technical Support

Technical support for DMS hardware and software will be provided by the LCC's and the software vendors (in accordance with their DMS contracts). Technical support for the command LANs will be the responsibility of NPS in accordance with pending NPS DMS policy. DISA will also man help desk to provide technical support for user customers [Ref. 12].

6. Personnel

Manning requirements for the SSTL will remain unchanged, therefore costs for additional personnel will not be incurred.

The SSTL will have to incur the expense of the absence of the SA while attending the four day DMS Orientation Course. Since this course will be held locally, there will be no expense for SA travel.

VIII. CONCLUSIONS

As discussed in Chapter VI, GCCS AMHS has the advantage over DMS in that the system has been tested, it is currently operational throughout DoD, and the applications are installed in the SSTL. However, GCCS AMHS is not fully functional, in the SSTL, due to the lack of AUTODIN connectivity. The DoN DMS Master Plan has AUTODIN scheduled for complete closure no later than 31 December 1999.

Although it is still evolving (as all technologies should), DMS is the better system for the SSTL. DMS requires less equipment, automates more processes, and provides better security of messages than GCCS AMHS. DMS is designed to accommodate legacy systems such as AUTODIN and front end systems such as GCCS AMHS. Under the circumstances, because AUTODIN installation is infeasible, the SSTL has no choice but to wait for DMS.

As DISA begins to implement DMS at the command levels, users must be prepared to adapt to the changes DMS will bring in order to reap its benefits This chapter will discuss the benefits of DMS implementation in the NPS SSTL and the cultural changes that will affect all DMS users.

A. BENEFITS OF DMS IMPLEMENTATION IN THE SSTL

This section discusses compatibility, adaptability, interoperability, training, and costs as major benefits of DMS implementation in the SSTL.

1. Compatibility

One of the key objectives of DMS is to make available to the user, compatible hardware and software products. The DMS-compliant certification program ensures that vendors products remain compatible with the system. The certification program will aid the SSTL in selecting vendors products based on the lab's own criteria (e.g., price, product functionality, ease of use, reputation).

2. Adaptability

DMS is designed to be flexible enough to adapt to the rapidly changing technology that is characteristic of the computer industry. The use of COTS products is encouraged to promote competition. With competition comes new technologies and capabilities for the DMS, as long as evolving technologies can be DMS certified. For the SSTL, emerging technology may include development of DMS products that have features tailored specifically for GCCS.

3. Interoperability

DII is the DoD's answer to ensure interoperability between its services, agencies, and U.S. allies. For the SSTL, this means that DMS will operate with GCCS and any other C4I systems it may later acquire that use the DII COE.

4. Training

DMS will be used DoD-wide and therefore, all service members must learn to use the system. CNET is reviewing many options to train all Navy personnel as DMS users. These options include assigning DMS basic user courses as part of the standard transfer order process, providing each LCC with a trainer who would conduct DMS user training for base level commands, or the use of computer based training. As DMS use becomes more extensive in the Navy, the SSTL will see more previously trained users. Users will be able to spend less time learning DMS more time training to use GCCS's other applications.

5. Costs

DMS will allow the SSTL to spend its funding on other areas of the lab. DISA and the DoN will fund the infrastructure, including DMS specific hardware and software requirements. NPS will fund LAN upgrade and connectivity expenses. This infrastructure will relieve the SSTL of the cost related to maintaining and monitoring the GCCS AMHS. DMS funding at the NPS level is still in the planning stages, therefore it is unclear as to what cost, if any, the SSTL will have to incur.

The implementation of DMS will also eliminate the cost of time the GCCS SA must commit to perform additional duties as the AMHS administrator and operator.

B. CULTURAL CHANGES

Technology changes bring about cultural changes as well. DMS is no exception. In an interview with Lieutenant General Edmonds,[15] when asked the question "What do you see as the main roadblock to timely implementation?" he replied:

> In two words, user acceptance. Any time we introduce a new technology, people must change their work habits, their way of thinking about who they are and what they do and how they get their work done. In short, user acceptance is difficult any time it requires a cultural change, and it takes some time to get it introduced.... DMS will provide organizations with the capability to prepare, coordinate, release, transmit, receive, and distribute organizational messages electronically. DMS will eliminate the requirement for specially skilled communications personnel to manually handle each message. Users must understand this new capability and determine how it can best be used in their organizations to improve productivity.

Some of the specific cultural changes that will occur with the implementation of DMS include:

- Carrying the Fortezza card will become as important as carrying a Military ID card.
- Standardized Message Formats will eliminate the guess-work and conflicts that often occur in joint commands.
- Departments within organizations or commands will be responsible for transmitting their own organizational messages.
- Individuals will be able to send classified E-mail to users within DoD and the government worldwide as a matter of routine

---

[15]LTG Edmonds is the Director of DISA and Manager, National Communications System (NCS). He is responsible for providing C4IFTW support. His interview can be found on page 5 of [Ref. 23].

The NPS and the SSTL will have to develop policies for users and staff that reflect these changes.

IX. RECOMMENDATIONS

After years of planning, testing, and talking, the DoD is moving faster and closer to making the Defense Message System a reality. Selected sites are scheduled to transition to DMS starting January 1997. NPS is scheduled to be fully operational by January 1999. Detailed yet easy to implement transition strategies, patience, and optimistic cooperation between DISA, the DoN PMO and NPS will improve our ability to take advantage of DMS. The remainder of this study discusses ways in which NPS can make use of time until NPS DMS implementation, areas of further study, and closing remarks.

A. WAITING FOR DMS

The mandated AUTODIN phase-out gives the SSTL no choice but to wait for DMS. The Navy's DMS PMO will coordinate AUTODIN ASC closure with the implementation of DMS at NPS. Detailed plans and coordination between NPS and the PMO are required to ensure a steady transition. While NPS waits for the DoN DMS PMO to finalize its DMS fielding schedule (with the final approval of DISA, Joint Chiefs of Staff (JCS), and the CINCs), the SSTL could take the following action:

- Seek representation for input to the NPS DMS Implementation Plan.
- Propose the SSTL as the NPS test site or "first to receive" site for the implementation of DMS SECRET message capability (i.e., Fortezza+ cards).
- Plan for absorbing DMS overhead duties into SSTL manning Plan.
- Decide where and how DMS architecture will co-reside with existing SIPRNET and SECRET LAN.
- Decide how many UA's to make available as DMS stations.
- Decide how many Fortezza users to support.

Once DMS is operational in the SSTL, the IAC could propose the SSTL's GCCS site as a research facility for GCCS/DMS interoperability projects and test site for new GCCS/DMS capabilities. This facility would be available for DISA, DoN, and NPS research or test and evaluation activities.

B. AREAS OF FURTHER STUDY

This thesis focused on the examination of GCCS AMHS and DMS and their interoperability with GCCS in an effort to determine the feasibility of the two messaging technologies for the SSTL. As technologies that are designed to evolve with changing technology, DMS and GCCS provide other areas for further study:

1. **DMS and GCCS mobile capability.** What are the roles of GCCS and DMS in the DII tactical/theater context? In transit (on ships)? Mobility for Marines?

2. **Multi-level security for GCCS and DMS**. How will multi-level security evolve to provide the required level of security for DMS and GCCS? Is the security tamper proof? Will there be a single security product (i.e. one type of Fortezza card) adequate enough to provide protection for DMS?

3. **GCCS and the DII COE.** What changes must occur for GCCS to adopt the DII COE? When are these changes scheduled to take place? What version of GCCS is expected to incorporate these changes? What does it mean for the SSTL?

4. **DMS policy for the SSTL.** As a classified enclave, will the SSTL need to establish its own Standard Operating Procedures (SOP) or will NPS set the policy? What will be required of the GCCS systems administrator? What criteria will be used to assign users Fortezza+ cards?

C. CLOSING REMARKS

The goal of this thesis is to present the SSTL with an analysis of two messaging technologies for the Global Command and Control System and the circumstances that make one (DMS) dominant, in terms of selection, over the other. Although neither systems are currently available for implementation in the SSTL, the

recommendation for DMS is heavily influenced by the fact that DMS is the target architecture for the DoD's messaging capability while GCCS AMHS (and its reliance on the outdated AUTODIN backbone) is the legacy system.

LIST OF REFERENCES

1. "He's Helping DoD' Parts Fit Together: An Interview with RADM John Gauss," Government Computer News, Cahners Publishing Company, Newton, MA, 4 March 1996.
2. "Defense Plans: A Sensitive Operation on its C4 Network," Government Computer News,Cahners Publishing Company, Newton, MA, 4 March 1996.
3. "Global Command and Control System: System and Network Management Concept of Operations," Version 1.6, Submitted by DISA Joint Interoperability and Engineering Organization (GCCS Engineering Department), 14 September 1995.
4. "Global Command and Control System Automated Message Handling System Administration," Manual for Soloris, Jet Propulsion Laboratory, California Institute of Technology, Pasadena , CA, 26 January 1995.
5. Hice, G.F. and Wold, S.H., "DMS: Prologue to the Government E-mail Revolution," J.G. Van Dyke & Associates, Inc., Bethesda, MD , 1995.
6. "DoN DMS Master Plan (Draft)," DMS Program Management Office PMW152, 12 August 1996.
7. "The Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS)," Prepared by DMS Transition Working Group, Office of the Assistant Secretary of Defense for C3I, November 1994.
8. "On the Job Training Handbook for the SPAWARE Automated Message Processing Message Dissemination Subststem (MDS): End User," Published by direction of Commander, Space and Naval Warfare Systems Command (PMW 152), Washington, DC, February 1993.
9. McGonigle, Myles, ET2, USN, NPS Classified Materials Manager, Interview 26 August 1996.
10. "GCCS Automated Message Handling System," 81st Training Group, 333d Training Squadron, Keesler AFB, MS 39534-2402, October 1995.
11. Norman, David, Director, Computer Services, NPS, Interview, July 1995.
12. Curry, C.M., "DMS Training Available on Many Levels," Chips Online, (http://www.chips.navy.mil), January 1996.

13. Porter, Gary, Research Assistant Prof. Joint C4I, NPS, Interviews, December 1995 - October 1996.

14. Joint Chiefs of Staff, MJCS-20-89, "Multi-command Required Operational Capability for the Defense Message System,: MROC 3-88," (http://www.disa.mil/D2/DMS/docs/mroc/mroc.html), 6 February 1989, Change 1, 4 August 1993.

15. "DMS Functional Requirements Document (FRD)," Prepared by Booz-Allen & Hamiliton Inc., 23 February 1995.

16. Paige, Emmit, Jr., Assitant Secretary of Defense (Command, Control, Communications, and Intelligence), "Guest Editorial," Chips Online, (http://www.chips.navy.mil), January 1996.

17. "Defense Information Infrastructure Master Plan Version 4.0," Defense Information Agency, for the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, .26 April 1996.

18. Loral, Product Ordering Guide, http://www.dms.loral.com.

19. Toler, Phil, LTCOL, "DMS: Order Processing Information," Chips Online, (http://www.chips.navy.mil, .January 1996.

20. DMS Frequently Asked Questions (FAQ), Navy DMS Homepage, www.spawar.navy.mil, 14 September 1996.

21. Emery, James, Assistant Provost, NPS (O5), Class Lecture (IS4182), 11 September 1996.

22. Garry, James, Naval Computer and Telecommunications Station, San Diego, (N5), Telephone Interview, 27 September 1996.

23. Edmonds, Lieutenant General, USAF, "Interview with LTG Albert J. Edmonds," Chips Online, (http://www.chips.navy.mil), January 1996.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road., Ste 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. Chairman, Department of Systems Management 1
   Code SM
   Naval Postgraduate School
   Monterey, CA 93943-5000

4. Chairman, Joint C3 Academic Group 1
   Code CC
   Naval Postgraduate School
   Monterey, CA 93943-5000

5. Prof. Gary Porter 3
   Code CC/Po
   Naval Postgraduate School
   Monterey, CA 93943-5000

6. Prof. Carl R. Jones 1
   Code SM/Jo
   Naval Postgraduate School
   Monterey, CA 93943-5000

7. Prof. Rex Buddenberg 1
   Code SM/Bu
   Naval Postgraduate School
   Monterey, CA 93943-5000

8. Mr. Hank Hankins 1
   Code CC
   Naval Postgraduate School
   Monterey, CA 93943-5000

9. Prof. James Emery 1
Code O5
Naval Postgraduate School
Monterey, CA 93943-5000

10. Mr. Dave Norman 1
Code SM
Naval Postgraduate School
Monterey, CA 93943-5000

11. LT Shenae Y. Morrow 2
7235 Caballero Avenue
Colorado Springs, CO 80911